4 二重化構成について

本章ではFirewallを2台使用して、二重化構成を構築するための手順について説明します。

セットアップの概要

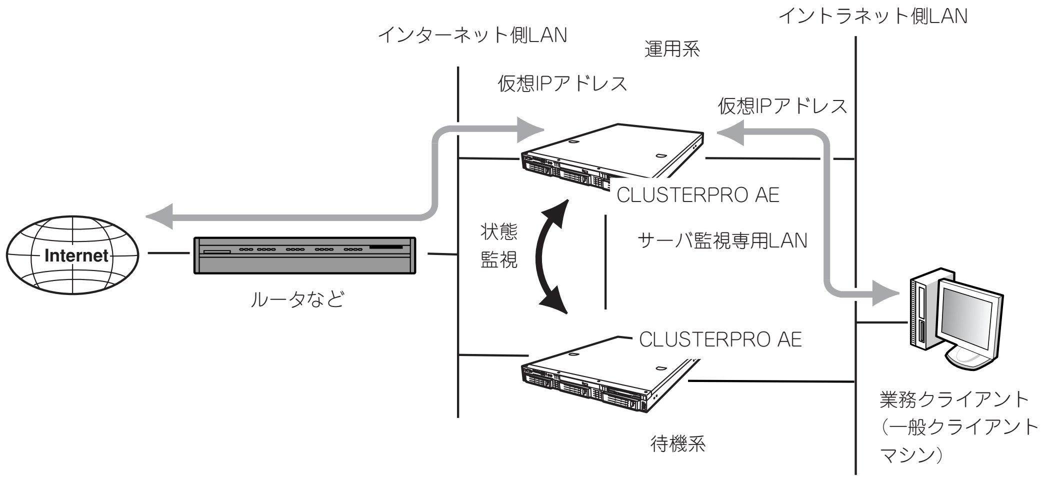
二重化構成について説明します。

動作概要

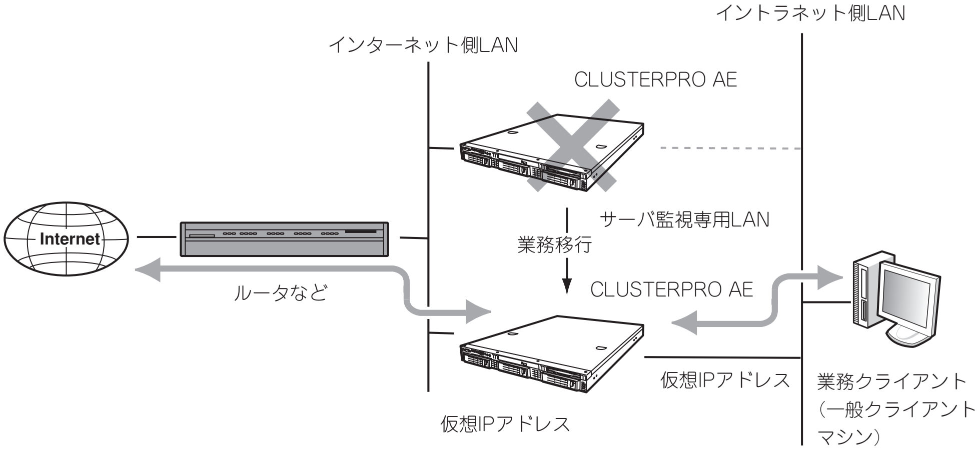
Firewallを二重化することで1台が障害などにより停止しても、もう1台のFirewallへ自動的に引き継ぐことにより、障害時の業務停止時間を最小限に抑えることができます。
また、運用系でFireWall-1のプロセスの異常を検出した場合や設定されたIPアドレスとの通信が途絶した場合にも、待機系に業務を引き継ぐことが可能です。

以下の仕組みでFirewallを二重化します。

- **通常運用時**
  - 運用系側のFirewallで有効にした仮想IPアドレスを使用してインターネット側とイントラネット側の双方からアクセスします。
  - 運用系/待機系のFirewallは互いにサーバの状態を監視をします。



- **運用系サーバ障害時**
  - 待機系のFirewallが運用系のダウンを検出します。
  - 運用系のFirewallが仮想IPアドレスを無効にします。
  - 待機系のFirewallが仮想IPアドレスを有効にします。
  - インターネット側とイントラネット側の双方からのアクセスは仮想IPアドレスを使用しているので業務の切り替わりを意識することはありません。



DMZを使用する場合もイントラネット、インターネット同様に仮想IPアドレスが引き継がれます。

構　成

二重化構成ではFirewall2台のほかに管理用サーバが必要となります。Express5800/FW300またはFW500をもう1台使用し、管理サーバとして動作させることも可能です。

必要なリソース

二重化を実現するためには、Firewallを単体で運用するときに比べて新たなリソースが必要です。
セットアップの前にリソースの計画や設定をしてください。

- **仮想IPアドレス(インターネット側): 1つ**

  インターネット側で引き継ぐアドレスです。

  インターネット側のネットワークアドレス内で未使用のIPアドレスを設定してください。

  このアドレスはFirewall本体のインタフェースに直接割り当てるアドレスではありません。

- **仮想IPアドレス(イントラネット側): 1つ**

  イントラネット側で引き継ぐアドレスです。

  イントラネット側のネットワークアドレス内で未使用のIPアドレスを設定してください。

  このアドレスはFirewall本体のインタフェースに直接割り当てるアドレスではありません。

- **仮想IPアドレス(DMZ側): 1つ**

  DMZで引き継ぐアドレスです。DMZを設けない場合には不要です。

  DMZのネットワークアドレス内で未使用のIPアドレスを設定してください。

  このアドレスはFirewall本体のインタフェースに直接割り当てるアドレスではありません。

- **Firewall間通信用アドレス: 1つ**

  Firewall間の監視に使用するアドレスです。

  基本的には、Firewall監視専用アドレスとして、Firewall本体のインタフェースに割り当ててください。

セットアップ

以下のネットワーク構成を例にとって設定を行います。

- **Firewall1（運用系）**

ホスト名:	fws1
インターネット側実IPアドレス:	202.247.5.1/255.255.255.0
DMZ側実IPアドレス:	172.16.1.1/255.255.255.0
イントラネット側実IPアドレス:	192.168.1.1/255.255.255.0
Firewall間通信用IPアドレス:	192.168.2.1/255.255.255.0

- **Firewall2（待機系）**

ホスト名:	fws2
インターネット側実IPアドレス:	202.247.5.2/255.255.255.0
DMZ側実IPアドレス:	172.16.1.2/255.255.255.0
イントラネット側実IPアドレス:	192.168.1.2/255.255.255.0
Firewall間通信用IPアドレス:	192.168.2.2/255.255.255.0

- **仮想IPアドレス**

インターネット側:	202.247.5.3
DMZ側:	172.16.1.3
イントラネット側:	192.168.1.3

- **プロキシARPアドレス**

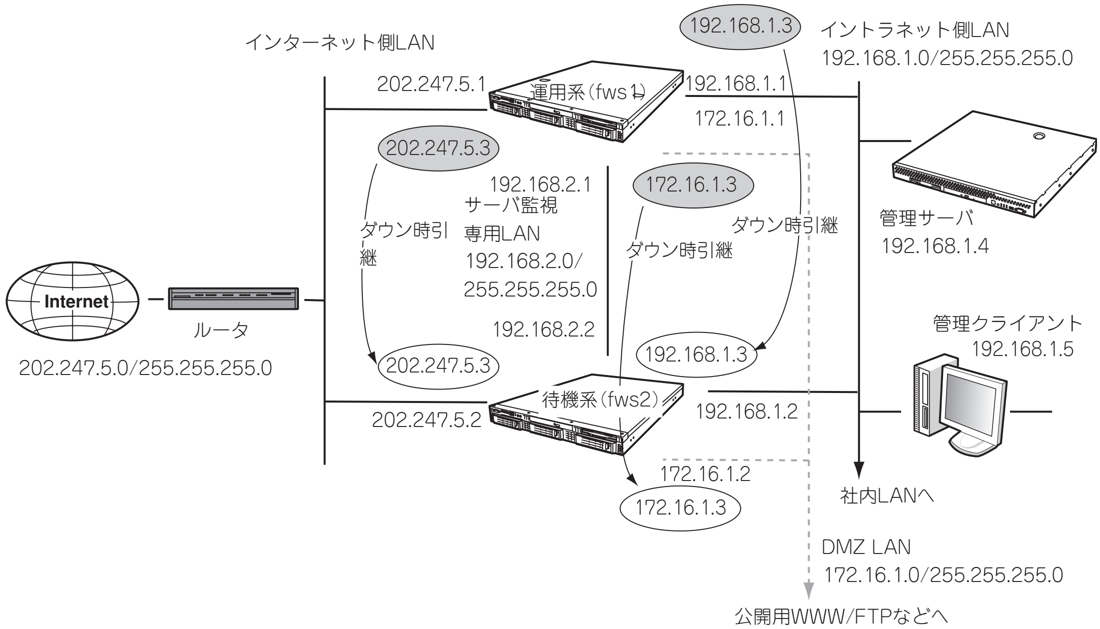
インターネット側:	202.247.5.4/255.255.255.0

- **管理用サーバ**

ホスト名:	firewall_mgr
IPアドレス:	192.168.1.4/255.255.255.0

- **GUIクライアント用PC**

IPアドレス:	192.168.1.5/255.255.255.0



設定手順の流れ

以下に設定手順の流れを示します。ここでは二重化に関する設定内容を説明します。その他の手順については3章を参照してください。

FireWall-1管理サーバのセットアップ

1. FireWall-1管理サーバの設定

↓

2. FireWall-1管理モジュールのコンフィグレーション

⇩

Firewall本体のセットアップ

1. マシンの設定

↓

2. FireWall-1のコンフィグレーション

⇩

セキュリティポリシーの設定

⇩

二重化機能の設定

⇩

他のネットワーク機器の設定

FireWall-1管理サーバのセットアップ

二重化する2台のサーバを管理するための管理サーバをセットアップします。以下の条件を満たすコンピュータに管理モジュールをインストールしてください。Express5800/FW300またはFW500をもう1台用意し、管理サーバとして動作させることも可能です。

オペレーティングシステム: Windows 2000 Server(SP1、SP2、SP3、SP4)、
Windows 2000 Advanced Server(SP1、SP2、SP3、SP4)、
Windows 2003 Server(SP1, SP2)、
Solaris8 / UltraSPARC、
Solaris9 / UltraSPARC、
Solaris10 / UltraSPARC、
RedHat Enterprise Linux 3.0 (kernel version 2.4.21)

Windows

ディスク容量: 300MB以上
メモリ: 256MB以上

Linux

ディスク容量: 300MB以上
メモリ: 256MB以上(推奨512MB以上)

Solaris

ディスク容量: 100MB以上
メモリ: 128MB以上(推奨256MB以上)

* 上記は、2007年3月現在の情報です。今後のパッチリリースにより変更になる可能性があります。

FireWall-1管理サーバの設定

Express5800/FW300またはFW500を管理サーバとして動作させる場合の設定例です。以下の手順に従って設定を行ってください。

1. インストール/初期導入設定ディスクによる設定を行う。

   3章の「1.インストール/初期導入設定用ディスクによる設定」を参照し、初期設定と管理クライアントの接続を行ってください。

   重要

   「インストール/初期導入設定用ディスクの作成」-「各入力項目の設定」において、「サーバタイプ」は「管理サーバ」にチェックをしてください。

2. 基本設定ツールによる設定を行う。

   重要

   3章の「2.システムのセットアップ」-「基本設定ツールによる設定」を参照し、管理サーバとして使用するための設定を行ってください。サーバタイプの設定では、「2. ManagementServer」管理サーバになっていることを確認してください。

```
# fwsetup

Firewall Server configuration tool Ver.2.4-2

server type
  1. Firewall
  2. Management Server
select number[2] ……………………………… 確認
      :
    〈略〉
      :
# shutdown -r now
```

3. 設定終了後、再起動する。

FireWall-1管理モジュールのコンフィグレーション

管理モジュールを管理サーバへインストールします。以下の手順でコンフィグレーションを行ってください。図中の〈略〉の設定する項目については、3章の「2. システムのセットアップ」-「FirewWall-1のコンフィグレーション」を参照してください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...  ......................... ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y  ........ ②

Please select one of the following options:
Check Point Power - for headquarters and branch offices.
Check Point UTM - for medium-sized businesses.
------------------------------------------------------------------

(1) Check Point Power.
(2) Check Point UTM.

Enter your selection  (1-2/a-abort) [1]: 2  ......................... ③

Please specify the Check Point UTM Product type you are about to install:
-------------------------

(1) VPN-1 UTM Gateway.
(2) SmartCenter UTM.
(3) SmartCenter UTM and VPN-1 UTM Gateway.

Enter your selection  (1-3/a-abort) [1]: 2  ......................... ④
```

① FireWall-1管理モジュールのコンフィグレーションをする。

② 使用許諾に承認した場合は<Y>キーを押す。

③ インストールする製品を選択する。

2 の「Check Point UTM」を選択し、インストールします。

④ インストールするモジュールを選択する。

「2」を選択し、インストールします。

```
            :
          （略）
            :
************* Installation completed successfully *************

Do you wish to start the installed product(s) now? (y/n) [y] ? y  ......①
cpstart: Power-Up self tests passed successfully
            :
          （略）
            :

# shutdown -r now  ......②
```

① 管理モジュールを起動させる。

② 再起動する。

Firewall本体のセットアップ

Firewallのセットアップについて説明します。

マシンの設定

以下の手順に従って設定を行ってください。

1. インストール/初期導入設定用ディスクによる設定を行う。

   3章の「1.初期導入設定用ディスクによる設定」を参照し、初期設定と管理クライアントの接続を行ってください。

2. 基本設定ツールによる設定を行う。

   3章の「2. システムのセットアップ」-「基本設定ツールによる設定」を参照し、設定を行ってください。

   重要

   上記の設定においては、二重化機能を使用しない設定としてください。二重化機能の設定につきましては、後述の「二重化機能の設定」で行います。

```
Use cluster system? (y/n) [n]: n
```

FireWall-1のコンフィグレーション

二重化構成の場合、コンフィグレーション手順が3章とは一部異なります。図中の〈略〉の設定する項目については、3章の「2. システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

① FireWall-1のコンフィグレーションをする。

② 使用許諾に承認した場合は<Y>キーを押す。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...  ........................ ①
               :
               :
               :
Do you accept all the terms of this license agreement (y/n) ? y  ........ ②

Please select one of the following options:
Check Point Power - for headquarters and branch offices.
Check Point UTM - for medium-sized businesses.
-------------------------------------------------------------------

(1) Check Point Power.
(2) Check Point UTM.

Enter your selection  (1-2/a-abort) [1]: 2  ........................ ③

Please specify the Check Point UTM Product type you are about to install:
-------------------------

(1) VPN-1 UTM Gateway.
(2) SmartCenter UTM.
(3) SmartCenter UTM and VPN-1 UTM Gateway.

Enter your selection  (1-2/a-abort) [1]: 1  ........................ ④
```

③ インストールする製品を選択する。

2 の「Check Point UTM」を選択し、インストールします。

④ インストールするモジュールを選択する。

「1」を選択し、インストールします。

① Dynamically Assigned IP Address Moduleをインストールするか問い合わせがあるので、<Enter>キーを選択する。

```
Is this a Dynamically Assigned IP Address gateway installation ? (y/n) [n] ? ............①
Would you like to install a Check Point clustering product (CPHA, CPLS or State
Synchronization)? (y/n) [n] ? y .................................................②

IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default Filter will be applied during boot.
This program will guide you through several steps where you
will define your Check Point products configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
                                    :
                                  (略)
                                    :
```

② Check Point clustering productをインストールするか問い合わせがあるので、<Y>キーを押す。

① FireWall-1管理サーバとFirewall間での通信に使用するパスワードを設定してください。

② 終了後、再起動します。

```
                                        :
                                      （略）
                                        :
Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized
Enter Activation Key:  ┐
Retype Activation Key: ┘ ............................................ ①

The Secure Internal Communication was successfully initialized

initial_module:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y ................................ ②
```

セキュリティポリシーの設定

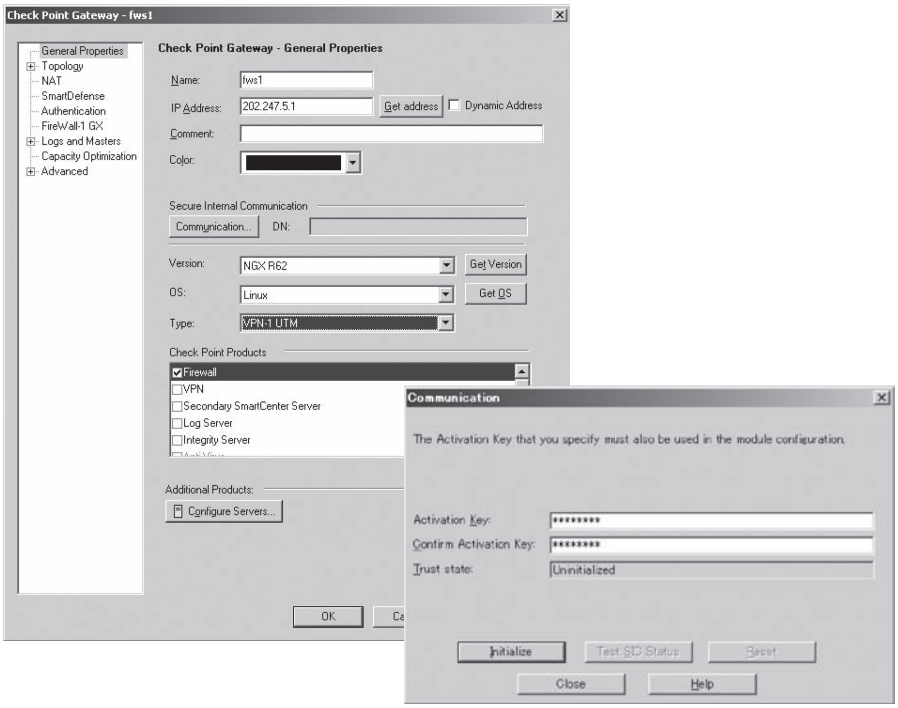
Firewallオブジェクトの作成

1. 2台のFirewallのオブジェクトを作成する。

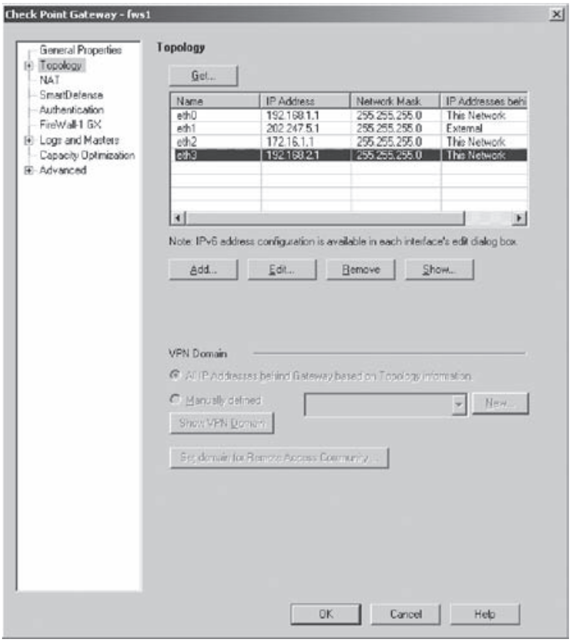
　― ViewObjectTreeの[CheckPoint]を選択し、右クリックします。
　　[New Check Point]→[VPN-1 Power/UTM Gateway]を選択します。
　　[Check Point installed Gateway using]ダイアログが表示された場合、[Classic mode]を選択し、[OK]を押してください。

　― オブジェクト：Gateway
　　名前　　　　：fws1、fws2
　　内容　　　　：IP AddressにはFireWall-1管理サーバと同じネットワークの実IPアドレスを設定してください。

　― FireWall-1管理サーバからFirewallを管理（セキュリティポリシーの設定やログ表示など）するためには、FireWall-1管理サーバとFirewallとの間で通信を行うための設定が必要です。Generalページで[Communication...]をクリックし、FireWall-1のコンフィグレーション時に設定したパスワードを入力してください。



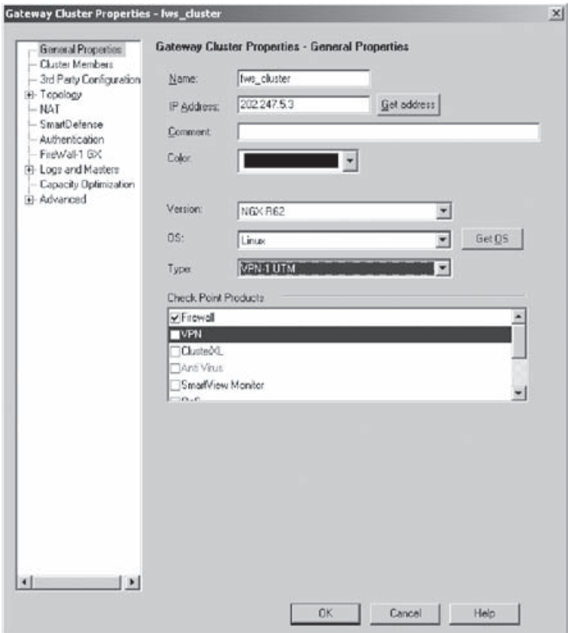
― Topologyページで全インタフェースを設定します。



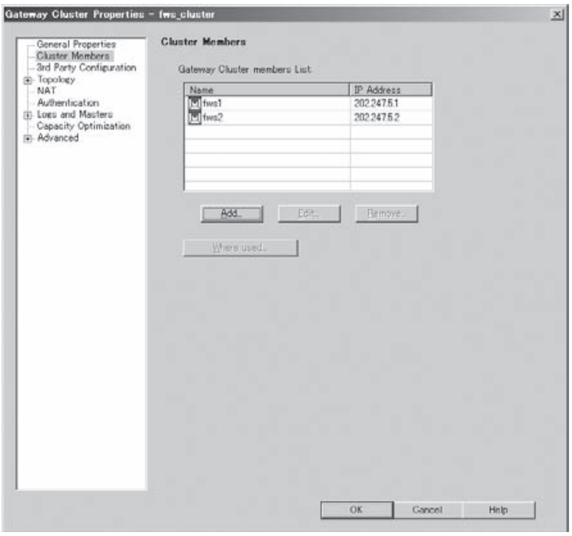
2. 以下のクラスタオブジェクトを作成する。

― ViewObjectTreeの[CheckPoint]を選択し、右クリックします。
[New Check Point]→[VPN-1 Power/UTM Cluster]を選択します。
[Check Point installed Gateway using]ダイアログが表示された場合、[Classic mode]を選択し、[OK] を押してください。

― オブジェクト : Gateway Cluster
名前 : fws_cluster
内容 : IP Addressにはインターネット側の仮想IPアドレスを指定してください。



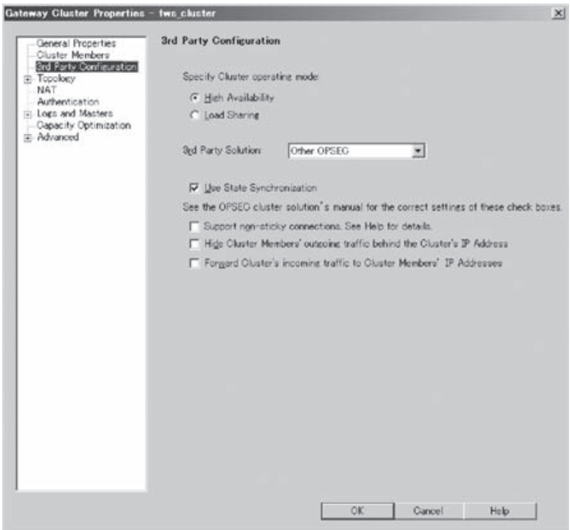
3. Cluster Membersページで、手順1で作成した2台のFirewallオブジェクト(fws1とfws2)を追加する。



4. 3rd Party Configurationページで、設定を確認する。

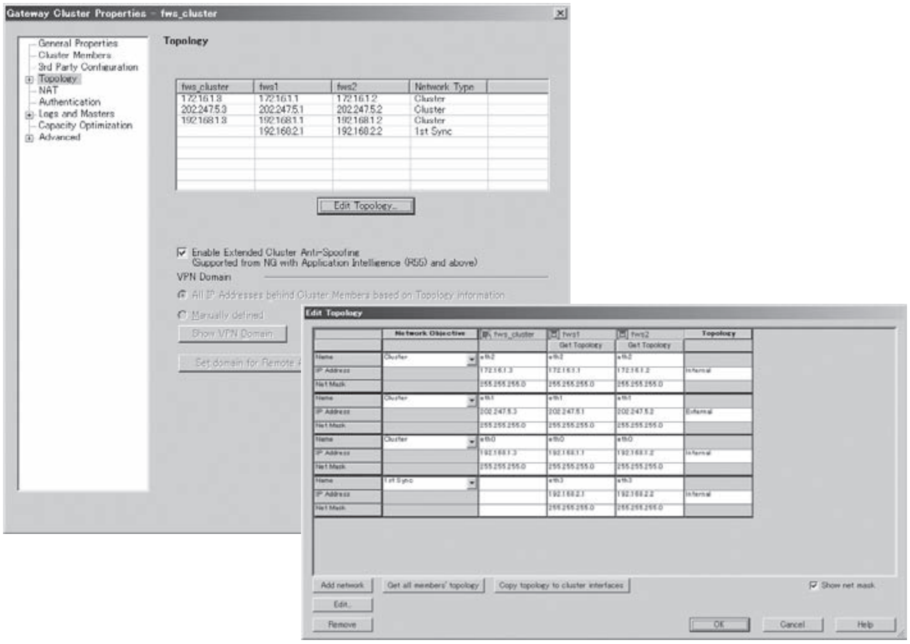
「Use State Synchronization」にチェックが付いていることを確認します。チェックが付いていない場合は、チェックを付けます。

「Hide Cluster Members' outgoing traffic behind the Cluster's IP Address」にチェックが付いていないことを確認します。



5. Topologyページにてインタフェースの設定をする。

[Edit Topology]をクリックします。
IPアドレスには、仮想IPアドレスを設定し、Network Objectiveプルダウンメニューより、「Cluster」を設定します。
同期用ネットワークのIPアドレスは設定せず、プルダウンメニューより、「1st Sync」を設定します。

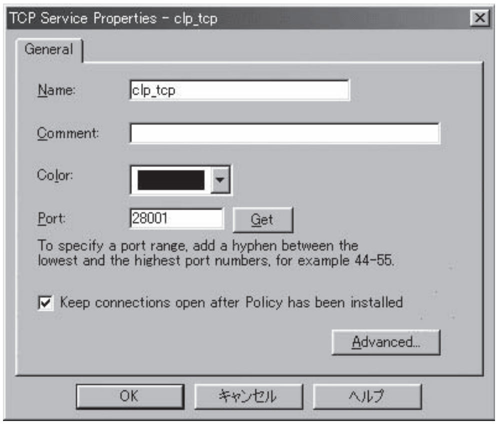


二重化用ルールの追加

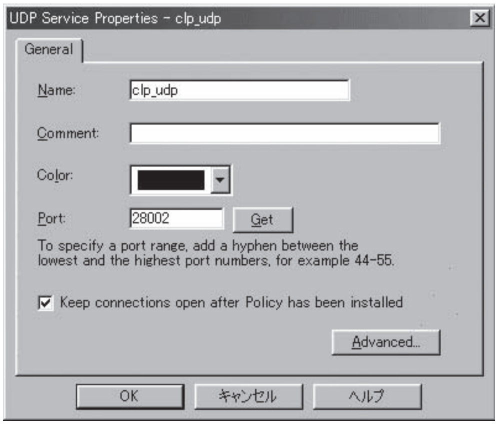
二重化機能を使用するためには、サーバ間の状態監視用通信を通すためのルールを設定する必要があります。

1. メニューの[Manage]→[Services...]→[New]を選択し、以下のサービスを定義する。(名前は一例です。他の名前でも構いません。)

   オブジェクト:TCP
   名前　　　　:clp_tcp
   ポート　　　:28001



   オブジェクト:UDP
   名前　　　　:clp_udp
   ポート　　　:28002



重要

上記ポート番号は基本設定ツールにおける既定値のポート番号です。二重化機能の設定でポート番号を変更する場合はその設定に合わせてサービスの定義を行ってください。

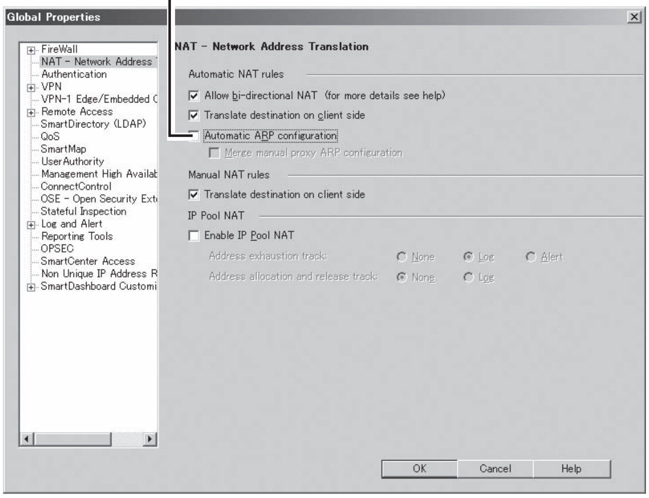
2. 上記の二重化通信用のルールを追加する。

項目	設定値
Source	:fws1、fws2
Destination	:fws2、fws1
Service	:clp_tcp、clp_udp
Action	:accept

二重化用設定事項

二重化機能を使用するためには、設定事項として、[Policy] - [Global Properties] - [NAT - Network address translation]ページで「Automatic ARP configuration」のチェックを外す必要があります。

チェックを外す



セキュリティポリシーのインストール

セキュリティポリシーの作成が完了したら、ポリシーをインストールしてください。2台のFirewallにインストールされます。

セキュリティポリシーのバックアップ

二重化構成の場合、ポリシー情報はFireWall-1管理サーバに保存されますが、情報のリストアの際には、管理サーバとFirewall本体の両方のバックアップデータが必要となります。管理サーバとしてExpress5800/FW300またはFW500を使用している場合には、3章の「4. バックアップ」コマンドによるバックアップを参照してください。FireWall-1モジュールのバックアップ方法と同じです。
その他のサーバを使用している場合には、該当するファイルのバックアップが必要となります。（以下のバックアップファイル取得方法は、Windowsマシンを使用した場合の一例です。）

1. コマンドプロンプトより、FireWall-1を停止させる。

```
C:¥> cpstop
```

2. 停止後、以下のコマンドを実行する。

   「export.tgz」バックアップファイルが作成されます。

```
C:¥> cd C:¥WINNT¥FW1¥R62¥fw1¥bin¥upgrade_tools
    > upgrade_export.exe export
```

> チェック
> 「C:¥WINNT¥FW1¥R62¥fw1」は、FireWall-1をインストールしたディレクトリになります。インストールディレクトリによって異なります。

3. バックアップファイルを取得後、FireWall-1を起動します。

```
C:¥> cpstart
```

> 重要
> **セキュリティポリシーの設定の説明において使用している画像イメージは、FireWall-1のFeaturePackによって異なる場合があります。**

二重化機能の設定

二重化機能の設定方法を説明します。設定は基本設定ツールから行います。両Firewallで全く同じ設定を行ってください。
二重化機能の設定項目およびそれぞれの制限事項は以下のとおりです。

- **ハートビート送信間隔**

  ハートビートの送信間隔(秒)を指定します。

- **ハートビートタイムアウト時間**

  ハートビートが途絶して相手Firewallがダウンしたと認識するまでの時間(秒)を指定します。ハートビート送信間隔より大きい値を指定してください。

- **Firewall起動待ち時間**

  起動時に相手Firewallの起動時間を待ち合わせる時間(秒)を指定します。ハートビートタイムアウト時間より大きい値を指定してください。

- **内部通信用TCPポート番号**

  2台のFirewall間で通信を行うためのTCPのポート番号を指定します。

- **内部通信用UDPポート番号**

  2台のFirewall間で通信を行うためのUDPのポート番号を指定します。

- **Firewall1のサーバ名**

  ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

- **Firewall2のサーバ名**

  ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

- **Firewall1のインタコネクトアドレス**

  相手Firewallを監視するためのアドレスとネットマスクを入力します。

- **Firewall2のインタコネクトアドレス**

  相手Firewallを監視するためのアドレスとネットマスクを入力します。

- **仮想IPアドレス**

  二重化機能を使用する場合、Firewallへのアクセスは原則仮想IPアドレスを使用する必要があります。

  サーバ間監視専用インタフェースを除く全インタフェースに仮想IPアドレスを設定してください。

- **監視対象アドレス**

  監視対象として設定されたIPアドレスとの通信が途絶した場合、待機系Firewallにフェイルオーバが行われます。本項目の設定は省略することができます。

- **プロキシARPアドレス**

  StaticNAT機能を使用する場合、外部公開アドレスとして使用するアドレスを指定してください。

● **運用系Firewall**

運用系のFirewallを指定します。

● **自動フェイルバック**

自動フェイルバックを行うかどうか設定します。自動フェイルバックをautoにした場合、運用系ダウン後、待機系に業務が引き継がれている状態で、運用系が復帰(起動)すると、自動的に運用系に業務を戻します。

基本設定ツールでの設定手順を示します。以下の内容は、本章の「セットアップ」で示したネットワーク構成を例にとって説明します。

```
# fwsetup ............................................................ ①
Firewall Server configuration tool Ver.2.4-2
     :
    〈略〉 ............................................................ ②
     :
use cluster system? (y/n)[n]: y ...................................... ③
```

① 管理クライアントからFirewallの設定ツールであるfwsetupコマンドを起動する。

② 「use cluster system」の項目までは、<ENTER>キーを押して進み、設定内容を確認する。

```
---- START CLUSTERPRO configuration ----------------

CLUSTERPRO Configuration Tool Ver 1.0-4

---- cluster configuration -------------------------

Input HB interval(0 - 999)[0] : ...................................... ①

Input HB timeout(1 - 999)[1] : ....................................... ②

Input WAIT Timeout(1 - 999)[5] : ..................................... ③

Input API TCP port number[28001] : ................................... ④

Input HB UDP port number[28002] : .................................... ⑤

Input server1 host name : fws1 ....................................... ⑥

Input server2 host name : fws2 ....................................... ⑦
```

③ 二重化機能を使用する。<Y>キーを押す。

① ハートビート送信間隔(秒)を入力する。

② ハートビートタイムアウト時間(秒)を入力する。

③ 起動時に相手Firewallの起動を待ち合わせる時間(秒)を入力する。

④ 内部通信用のTCPポート番号を入力する。

⑤ 内部通信用のUDPポート番号を入力する。

⑥ Firewall1のサーバ名（ホスト名）を入力する。

ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

⑦ Firewall2のサーバ名（ホスト名）を入力する。

ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

```
---- server configuration ---------------------------

Input fws1 interconnect address ..................... ①
address(1) : 192.168.2.1
netmask(1) : 255.255.255.0
address(2) :
 No.  address/netmask
  1   192.168.2.1/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

Input fws2 interconnect address ..................... ②
address(1) : 192.168.2.2
netmask(1) : 255.255.255.0
address(2) :
 No.  address/netmask
  1   192.168.2.2/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 運用系FirewallのFirewall間監視用アドレス（インタコネクトアドレス）とネットマスクを入力する。

インタコネクトアドレスは16個まで設定可能です。

設定後に一覧を表示します。

一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter>キー:	インタコネクトアドレスを追加します。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正します。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除します。
<L>キー+<Enter>キー:	一覧を再表示します。
<Enter>キー:	次の項目へスキップします。

② 待機系FirewallのFirewall間監視用アドレス（インタコネクトアドレス）とネットマスクを入力する。

```
---- group configuration ------------------------------

 No.  name
  1   group0

---- group fip configuration ---------------------------

Input FIP address ······························ ①
address(1) : 202.247.5.3
netmask(1) : 255.255.255.0
address(2) : 172.16.1.3
netmask(2) : 255.255.255.0
address(3) : 192.168.1.3
netmask(3) : 255.255.255.0
address(4) :
 No.  address
  1   202.247.5.3/255.255.255.0
  2   172.168.1.3/255.255.255.0
  3   192.168.1.3/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 仮想IPアドレスを入力する。

仮想IPアドレスは8個まで設定可能です。

設定後に一覧を表示しますので、確認、または、変更して<Enter>キーで進みます。

ヒント

二重化機能を使用する場合、サーバへのアクセスは、原則仮想IPアドレスを使用する必要があります。
サーバ間監視専用インタフェース以外の全インタフェースに仮想IPアドレスを設定してください。

```
---- group0 ipw configuration ------------------------------

Input IPW address ………………………………………………………… ①
address(1) : 202.247.5.xxx |202.247.5.xxx
address(2) :
 No.  address
  1   202.247.5.xxx |202.247.5.xxx

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 監視するIPアドレスを入力する。

「|」で区切って複数のIPアドレスを入力することができます。その場合は、指定した全IPアドレスとの通信が途絶した場合にリソース異常となります。

監視するIPアドレスは8個まで設定可能です。ただし、「|」で区切ったIPアドレスは全体で1つのIPアドレスとしてカウントします。

設定後に一覧を表示しますので、確認、または、変更して<Enter>キーで進みます。

> ヒント
> 監視対象として設定されたIPアドレスとの通信が途絶した場合、待機系サーバにフェイルオーバが行われます。

<設定例>

- 202.247.5.254と192.168.1.254のどちらかと通信が途絶した場合にフェイルオーバを行いたい場合。

No.	address
1	202.247.5.254
2	192.168.1.254

- 202.247.5.254と192.168.1.254の双方と通信が途絶した場合にフェイルオーバを行いたい場合。

No.	address
1	202.247.5.254 | 192.168.1.254

- 202.247.5.5と202.247.5.254の双方と通信が途絶した場合か、192.168.1.254と通信が途絶した場合にフェイルオーバを行いたい場合

No.	address
1	202.247.5.5 | 202.247.5.254
2	192.168.1.254

```
---- group0 proxy arp configuration ------------------------------

Input proxy address ····························································· ①
address(1) : 202.247.5.4
address(2) :
 No.  address
  1   202.247.5.4

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 設定するプロキシアドレスを指定する。

プロキシARPアドレスを入力します。プロキシARPアドレスは256個まで設定可能です。

設定後に一覧を表示しますので、確認、または、変更して<ENTER>キーで進みます。

ヒント

プロキシARPアドレスでは、運用系サーバにてStaticNATを行う場合の公開用IPアドレスとなります。StaticNATで公開するIPアドレスを全て登録してください。

```
---- group0 resource configuration --------------------------

Input primary server hostname(fws1, fws2)[fws1] : ························ ①

Input failback policy(1:auto, 2:manual)[manual] : ························ ②

---- END CLUSTERPRO configuration -----------------

         :
        〈略〉
         :
```

① 運用系サーバを入力する。

② 自動フェイルバックを行うかどうか入力する。

重要

上記の設定はfws1、fws2で同じ設定にしてください。

上記の設定後は、本体を再起動させる必要があります。以下のコマンドを入力してください。

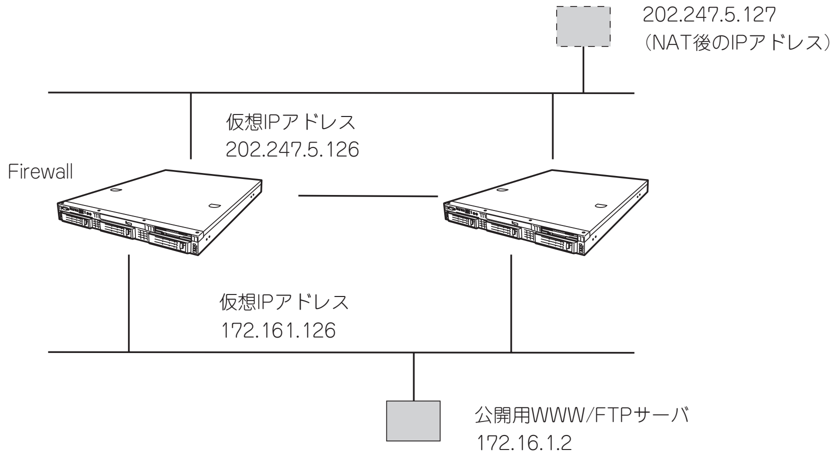
```
# shutdown -r now
```

他のネットワーク機器の設定

イントラネットとDMZに存在するネットワーク機器については、デフォルトルートの設定としてサーバに設定したそれぞれのネットワークの仮想IPアドレス（イントラネット側: 192.168.1.3、DMZ側: 172.16.1.3）を指定するようにしてください。

【参考】NATのためのルーティングテーブル

Firewallの二重化構成において、DMZ上やローカルネット内のサーバのアドレスを静的にNAT（アドレス変換）し、インターネット上に公開する場合、ルーティングテーブルとプロキシARPテーブルの設定を別途行う必要があります。
例として、以下のネットワーク構成の場合、公開用WWW/FTPサーバを該当するホストとすると、以下のようなルーティングテーブルとプロキシARPテーブルの設定をFirewallへ行う必要があります。



destination 202.247.5.127
netmask 255.255.255.255
gateway 172.16.1.2

変換後のアドレスをdestination、実際のアドレスをgatewayに指定してください。
fwsetupのstatic routingの項目で設定することができます。
プロキシARPの設定については、前述の「二重化機能の設定」を参照してください。

運　用

二重化構成の運用について説明します。

障害発生時の対応

運用系サーバにおいて障害を検出した場合には、フェイルオーバが発生し、待機系サーバへ業務が切り替わります。その際に基本設定ツールで指定した管理者のE-mailアドレス宛にメールが送信されます。

● ダウンしたときのメッセージ

```
Subject: WARNING: [group0] is downed

 !!WARNING!!
 [group0] is not active on Firewall(fws1.nec.co.jp[202.247.5.1]).
 Urgently check it.

 If you recieved a previous message "NOTICE: [group0] changes
 to the active firewall" from fws1.nec.co.jp[202.247.5.1],
 both groups are downed.
 Urgently check both groups!!
```

● フェイルオーバしたときのメッセージ

```
Subject: NOTICE: [group0] chnges to the active firewall

 !!NOTICE!!
 [group0] chnges to the active
 firewall(fws2.nec.co.jp[202.247.5.2]).
 Urgently check another failed firewall.
```

重要 **ダウンした要因がネットワークの通信障害などの場合、ダウンしたときのメッセージがサーバ内に滞留し、障害復旧後に送信されることがあります。メッセージを受信したら必ずその発信時刻を確認するようにしてください。**

メールを受信したらExpress5800/FW300の状態を確認し、システムログからフェイルオーバが発生した要因を確認し、必要な対処を行ってください。メッセージ内容、対処方法等は「付録C 二重化機能のログメッセージ」を参照してください。

- 監視対象IPアドレスとの通信途絶、あるいは、FireWall-1プロセス消滅が発生し、待機系Firewallに業務を引き継いだ場合、以後、そのサーバ上での業務の起動が拒否されるようになります。そのFirewallが業務の起動拒否状態かどうかは、[clpstat -s]の[STARTING]で確認できます。
- 運用系Firewallが起動拒否状態のまま待機系Firewallで業務を遂行している場合、待機系Firewallで監視対象IPアドレスとの通信途絶、あるいはFireWall-1プロセス消滅が発生しても、待機系Firewallから運用系Firewallへは業務が引き継がれず、引き続き待機系Firewallで業務が遂行されます。但し、上記の条件においても相互のインターコネクトの通信が途絶した場合においてはこの限りではなく、起動拒否状態であっても運用系Firewallで業務が遂行されます。起動拒否状態は、次の手順により解除されます。

[監視対象IPアドレスとの通信途絶が原因の場合]

- 監視対象IPアドレスとの通信復帰
- clpgrpコマンドによって業務を起動
- Firewall再起動

[FireWall-1プロセス消滅が発生した場合]

- clpgrpコマンドによって業務を再開
- Firewall再起動

コマンドリファレンス

状態表示、運用系、待機系の切替等はコマンドを使用して行います。

情報表示

現在の状態、設定内容を確認するには以下のコマンドを実行します。

```
clpstat -s [-h host_name]
        -n
        -i [-h host_name]
```

状態、設定情報の表示を行います。

〈オプション〉

-sまたは引数なし .... 各種状態を表示します。
-n .... インタコネクトマップを表示します。
-i .... 各種設定を表示します。
-h host_name .... 操作対象サーバ名。指定なしの場合、コマンド実行サーバが対象となります。

```
# clpstat -s

==================  CLUSTER STATUS  ==============
* server0 : fws1                     1.0-1.4   ① 
  server1 : fws2                               ②
                              server0  server1
 -------------------------------------------------
   SERVER STATUS ................... ONLINE  ONLINE   ③
   GROUP0 STATUS ................... ONLINE  OFFLINE  ④
     POLICY                           1st     2nd     ⑤
     STARTING ...................... ALLOW   DENY     ⑥
     <A> group0-ipw0                  ONLINE  ONLINE   ⑦
       192.168.1.254                                   ⑧
     <U> group0-fip0                  ONLINE  OFFLINE  ⑨
       202.247.5.3/255.255.255.0                       ⑩
     <U> group0-parp0                 ONLINE  OFFLINE  ⑪
       202.247.5.5                                     ⑫
     <U> group0-exec0                 ONLINE  OFFLINE  ⑬
       S: /opt/necfws/bin/ckcstat                      ⑭
       E: /opt/necfws/bin/ckcstat                      ⑮
     <U> group0-exec1                 ONLINE  OFFLINE
       W: /opt/necfws/bin/ckfwalive
       E: /opt/necfws/bin/ckfwalive -k

--------------------------------------------------
```

clpstat -sの各項目について

① サーバ名(1台目)
② サーバ名(2台目)
③ サーバの状態
ONLINE ：ハートビートが受信されている
OFFLINE ：ハートビートが受信されていない
④ グループの状態
ONLINE ：正常
OFFLINE ：停止
ERROR ：異常
UNKNOWN ：不明
⑤ フェイルオーバポリシ
⑥ グループ起動の許可/禁止
ALLOW ：許可
DENY ：禁止
UNKNOWN ：不明
⑦ IPWリソースの起動種別と状態
<A> ：全サーバ起動
<U> ：単サーバ起動
ONLINE ：正常
OFFLINE ：停止
ERROR ：異常
UNKNOWN ：不明
⑧ IPWリソース監視アドレス
⑨ FIPリソースの状態
※ IPWリソースと同様
⑩ FIPリソース設定アドレス/ネットマスク
⑪ PARPリソースの状態
※ IPWリソースと同様
⑫ PARPリソース設定アドレス
⑬ EXECリソースの状態
※ IPWリソースと同様
⑭ EXECリソース起動時実行パス
S ：監視なし
W ：監視あり
⑮ EXECリソース停止時実行パス

```
# clpstat -i

=================  CLUSTER INFORMATION  =============
 SERVER : fws1

 ---------------------------------------------------
 CLUSTER :
  STARTUP       : AUTO      ①
  WAIT timeout  : 5         ②
  HB port       : 24002     ③
  HB interval   : 1         ④
  HB timeout    : 5         ⑤
  API port      : 24001     ⑥
  API timeout   : 30        ⑦
  LOG port      : 0         ⑧
  ping timeout  : 3         ⑨
  RECOVER       : RESTART   ⑩
  RETRY count   : 5         ⑪

  SERVER0 : fws1            ⑫
   INTERCONNECT0  : 192.168.1.1/255.255.255.0   ⑬
   INTERCONNECT1  : 192.168.2.1/255.255.255.0

  SERVER1 : fws2            ⑭
   INTERCONNECT0  : 192.168.1.2/255.255.255.0   ⑮
   INTERCONNECT1  : 192.168.2.2/255.255.255.0

  GROUP0 : group0           ⑯
   START             : AUTO         ⑰
   FAILBACK          : MANUAL       ⑱
   ENVIRONMENT       : ACT_NORMAL   ⑲
   RECOVER           : IGNORE       ⑳
   RETRY count       : 0/0          ㉑
   FAILOVER policy   : 0:fws1 1:fws2   ㉒

   IPW0 : group0-ipw0       ㉓
    TYPE                : ASR             ㉔
    POLLING address     : 192.168.1.254   ㉕
    RECOVER             : FAILOVER        ㉖
    RETRY count         : 2/2             ㉗

   FIP0 : group0-fip0       ㉘
    TYPE                : USR             ㉙
    ADDRESS             : 202.247.5.3/255.255.255.0   ㉚
    INTERFACE           : eth0:1          ㉛
    PING count          : 0               ㉜
    ARP count           : 1               ㉝
    RECOVER             : RETRY           ㉞
    RETRY count         : 5/5             ㉟

   PARP0 : group0-parp0     ㊱
    TYPE                : USR             ㊲
    IP ADDRESS          : 202.247.5.5     ㊳
    MAC ADDRESS         : 00:A0:34:1A:4C:D3   ㊴
    INTERFACE           : eth0            ㊵
    PING count          : 0               ㊶
    ARP count           : 1               ㊷
    RECOVER             : RETRY           ㊸
    RETRY count         : 5/5             ㊹
```

<次ページに続く>

```
  EXEC0 : group0-exec0
   TYPE               : USR ......................................... ㊻
   ACT path           : /opt/necfws/bin/ckcstat ..................... ㊼
   DEACT path         : /opt/necfws/bin/ckcstat ..................... ㊽
   POLLING            : NO .......................................... ㊾
   PID                : 21623 ....................................... ㊿
   RECOVER            : STOP ........................................ 51
   RETRY count        : 0/0 ......................................... 52

  EXEC1 : group0-exec1
   TYPE               : USR
   ACT path           : /opt/necfws/bin/ckfwalive
   DEACT path         : /opt/necfws/bin/ckfwalive -k
   POLLING            : YES
   PID                : 21625
   RECOVER            : FAILOVER
   RETRY count        : 2/2

=====================================================
```

clpstat -iの各項目について

① CLUSTERPRO AE の起動方法
YES　　　　　：自動起動
NO　　　　　：手動起動
② 起動待ち合わせ時間(秒)
③ ハートビート受信用 UDP ポート番号
④ ハートビート送信間隔(秒)
⑤ ハートビートタイムアウト(秒)
⑥ API用 TCP ポート番号
⑦ APIタイムアウト(秒)
⑧ ログポート番号
⑨ pingコマンドタイムアウト(秒)
⑩ リカバリ方法
RESTART　　：CLUSTERPRO AE再起動
STOP　　　　：CLUSTERPRO AE停止
HALT　　　　：OSシャットダウン
REBOOT　　：OSリブート
UNKNOWN　：不明
⑪ リトライ回数
⑫ サーバ名(1台目)
⑬ インタコネクトアドレス
⑭ サーバ名(2台目)
⑮ インタコネクトアドレス
⑯ グループ名
⑰ グループ起動方法
AUTO　　　：自動
MANUAL　　：手動
UNKNOWN　：不明
⑱ フェイルバック方法
AUTO　　　：自動
MANUAL　　：手動
UNKNOWN　：不明
⑲ 環境変数
ACT_NORMAL　　　：通常起動
ACT_FAILOVER　　：フェイルオーバ
DEACT_NORMAL　　：通常停止
DEACT_ILLEGAL　　：異常停止
⑳ グループリカバリ方法
IGNORE　　：無視
RETRY　　　：再起動
STOP　　　：停止
FAILOVER　：フェイルオーバ
UNKNOWN　：不明
㉑ リトライ回数
㉒ 運用系サーバ名 待機系サーバ名
㉓ IPWリソース名
㉔ 起動タイプ
ASR　　　：全起動リソース
USR　　　：単起動リソース
㉕ IPWリソース監視対象アドレス
㉖ IPWリソースリカバリ方法
IGNORE　　：無視
RETRY　　　：再起動
STOP　　　：停止
FAILOVER　：フェイルオーバ
UNKNOWN　：不明
㉗ リトライ回数
㉘ FIPリソース名
㉙ 起動タイプ
※ IPWリソースと同様
㉚ FIPアドレス
㉛ FIPインタフェース
㉜ ping回数

㉝ arp回数
㉞ FIPリソースリカバリ方法
※ IPWリソースと同様
㉟ リトライ回数
㊱ PARPリソース名
㊲ 起動タイプ
※ IPWリソースと同様
㊳ PARPアドレス
㊴ MACアドレス
㊵ PARPインタフェース
㊶ ping回数
㊷ arp回数
㊸ PARPリソースリカバリ方法
※ IPWリソースと同様
㊹ リトライ回数
㊺ EXECリソース名
㊻ 起動タイプ
※ IPWリソースと同様
㊼ EXECリソース起動時実行パス
㊽ EXECリソース停止時実行パス
㊾ EXECリソース監視設定
※ IPWリソースと同様
㊿ EXECリソースプロセスID
51 EXECリソースリカバリ方法
※ IPWリソースと同様
52 リトライ回数

```
# clpstat -n

===========  INTERCONNECT INFORMATION  =============
 server0 : fws1 ........................................ ①
 server1 : fws2 ........................................ ②
 [on server0 : ONLINE] ................................. ③
 address            server0  server1
 ---------------------------------------------------
 192.168.1.1          OK       OK ...................... ④
 192.168.2.1          OK       OK ...................... ⑤

[on server1 : ONLINE] .................................. ⑥
 address            server0  server1
 ---------------------------------------------------
 192.168.1.2          OK       OK
 192.168.2.2          OK       OK
```

clpstat -nの各項目について

① サーバ名(1台目)
② サーバ名(2台目)
③ サーバ(1台目)ステータス
④ プライマリインタコネクトアドレス／ステータス
⑤ セカンダリインタコネクトアドレス／ステータス
⑥ サーバ(2台目)ステータス

運用系/待機系の切り替え・業務の起動/停止

運用系/待機系の切替や、業務の起動/停止を行う場合、以下のコマンドを実行します。

```
clpgrp -s  [-h host_name] [-g group_name]
       -t  [-h host_name] [-g group_name]
       -m  [-h host_name] [-g group_name]
```

業務の起動/停止関連操作を行います。

〈オプション〉

-s .... 業務の起動を行います。すでに起動されていたり、他のサーバで起動している場合には失敗します。

-t .... 業務の停止を行います。すでに停止されていたり、他のサーバで起動されている場合には失敗します。

-m .... 業務の実行サーバを切り替えます。業務が起動しているサーバ側で実行する必要があります。

-h host_name .... 操作対象サーバ名です。指定なしの場合、コマンド実行サーバが対象となります。-m オプション指定時には、業務移動元サーバの意味も持ちます。

-g group_name .... 操作対象グループを指名します。指定なしの場合、全グループが対象となります。

二重化構成の再セットアップ

二重化構成の場合の再セットアップについて説明します。
次の手順に従って再インストールします。

重要 **再インストールは、LANケーブルをすべてはずしてから実行してください。**

● **管理サーバ**

Express5800/FW300またはFW500を管理サーバにしている場合のFireWall-1管理サーバの再インストールについて説明します。

1. 3章の「再セットアップ」-「システムの再インストール」の手順5までを行います。

2. 起動後、CD-ROMドライブにCheck Point NGX CD-ROM (CD1) をセットし、FireWall-1のモジュールを以下の手順で適用します。

```
# mount /dev/cdrom
# cd /mnt/cdrom
# ./UnixInstallScript
```

3. [Welcome]画面が表示されますので、<N>キーで次に進みます。

4. 使用許諾書が表示されますので、お読みいただいた後、使用許諾に承認した場合は<Y>キーを押します。

5. 以下のメッセージが表示されます。<2>キーを入力し、<N>キーで次に進みます。

```
Check Point Power - for headquarters and branch offices
Check Point UTM - for medium-sized businesses

1 ( ) Check Point Power
2 (*) Check Point UTM
```

6. 以下のメッセージが表示されます。<1>キーを入力し、<N>キーで次に進みます。

```
Please select one of the following options

1 (*) New Installation
2 ( ) Installation Using Imported Configuration
```

7. 以下のメッセージが表示されます。<2>キーを入力し、<N>キーで次に進みます。

```
The following products are available in this version
Please select product(s)


1 [ ] VPN-1 UTM
2 [*] SmartCenter UTM
3 [ ] Eventia Reporter UTM
4 [ ] SmartPortal
```

8. インストールするプロダクトが表示されます。<N>キーを入力し、次に進みます。

```
You have selected the following products for installation:
* SmartCenter UTM
```

9. 以下のメッセージが表示されます。ここではライセンス入力しないため、<n>キーを入力し、<Enter>キーで次に進みます。

```
Configuring Licenses...
=======================
Host             Expiration  Signature                              Features

Note: The recommended way of managing licenses is using SmartUpdate.
cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [y] ? n
```

10. 以下のメッセージが表示されます。ここでは登録を実施しないため、<n>キーを入力し、<Enter>キーを入力します。継続するので、<y>キーを入力し、<Enter>キーを入力します。

```
Configuring Administrator...
============================
No Check Point products Administrator is currently
defined for this SmartCenter Server.

Do you want to add an administrator (y/n) [y] ? n

No administrator is currently defined.
Are you sure you want to continue? (y/n) [n] ? y
```

11. 以下のメッセージが表示されます。<n>キーを入力し、<Enter>キーで次に進みます。

```
Configuring GUI Clients...
==========================
GUI Clients are trusted hosts from which
Administrators are allowed to log on to this SmartCenter Server
using Windows/X-Motif GUI.

No GUI Clients defined
Do you want to add a GUI Client (y/n) [y] ? n
```

12. 以下のメッセージが表示されます。<Enter>キーを2回入力し、次に進みます。

```
Configuring Group Permissions...
================================

Please specify group name [<RET> for super-user group]:

No group permissions will be granted. Is this ok (y/n) [y] ?
```

13. 以下のメッセージが表示されます。<n>キーを入力し、<Enter>キーで次に進みます。

```
Configuring Certificate's Fingerprint...
========================================
The following text is the fingerprint of this SmartCenter Server:
AAAA AAA AAAA AAA AAA AAAA AAAA AAA AAAA AAAA AAAA AAAA

Do you want to save it to a file? (y/n) [n] ? n
```

14. 再起動をするか確認のメッセージが表示されます。ここでは、<E>キーを入力し、次に進みます。

```
Installation program completed


In order to complete the installation
you must reboot the machine.

Would you like to reboot the machine ?

NOTE: Please remove the CD from
          your machine before reboot.
```

15. CD-ROMを取り出し、再起動します。

```
# cd
# eject
# shutdown -r now
```

16. 3章の「再セットアップ」-「システムの再インストール」の手順20を行い、管理サーバへバックアップをリストアします。

● Firewall本体

Firewall本体の再インストール方法について説明します。

1. 3章の「再セットアップ」-「システムの再インストール」の手順5までを行います。

2. 起動後、CD-ROMドライブにCheck Point NGX CD-ROM (CD1) をセットし、FireWall-1のモジュールを以下の手順で適用します。

```
# mount /dev/cdrom
# cd /mnt/cdrom
# ./UnixInstallScript
```

3. [Welcome]画面が表示されますので、<N>キーで次に進みます。

4. 使用許諾書が表示されますので、お読みいただいた後、使用許諾に承認した場合は<Y>キーを押します。

5. 以下のメッセージが表示されます。<2>キーを入力し、<N>キーで次に進みます。

```
Check Point Power - for headquarters and branch offices
Check Point UTM - for medium-sized businesses

1 ( ) Check Point Power
2 (*) Check Point UTM
```

6. 以下のメッセージが表示されます。<1>キーを入力し、<N>キーで次に進みます。

```
Please select one of the following options

1 (*) New Installation
2 ( ) Installation Using Imported Configuration
```

7. 以下のメッセージが表示されます。<1>キーを入力し、<N>キーで次に進む。

```
The following products are available in this version
Please select product(s)


1 [*] VPN-1 UTM
2 [ ] SmartCenter UTM
3 [ ] Eventia Reporter UTM
4 [ ] SmartPortal
```

8. インストールするプロダクトが表示されます。<N>キーを入力し、次に進みます。

```
You have selected the following products for installation:
* VPN-1 UTM
```

9. 以下のメッセージが表示されます。<n>キーを入力し、<Enter>キーで次に進みます。

```
Welcome to Check Point Configuration Program
=================================================
Is this a Dynamically Assigned IP Address gateway installation ? (y/n) [n] ?
```

10. 以下のメッセージが表示されます。<y>キーを入力し、<Enter>キーで次に進みます。

```
Would you like to install a Check Point clustering product (CPHA, CPLS or State Synchronization)? (y/n) [n] ? y
IP forwarding disabled
```

11. 以下のメッセージが表示されます。ここではライセンス入力しないため、<n>キーを入力し、<Enter>キーで次に進みます。

```
Configuring Licenses...
=======================
Host             Expiration  Signature                            Features

Note: The recommended way of managing licenses is using SmartUpdate.
cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [y] ? n
```

12. 以下のメッセージが表示されます。<Enter>キーを2回入力し、次に進みます。

```
Configuring Group Permissions...
================================

Please specify group name [<RET> for super-user group]:

No group permissions will be granted. Is this ok (y/n) [y] ?
```

13. 以下のメッセージが表示されます。FireWall-1管理サーバとFirewall間での通信に使用するパスワードを設定してください。

```
Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized
Enter Activation Key:
Retype Activation Key:
```

14. 再起動をするか確認のメッセージが表示されます。ここでは、<E>キーを入力し、次に進みます。

```
Installation program completed


In order to complete the installation
you must reboot the machine.

Would you like to reboot the machine ?

NOTE: Please remove the CD from
          your machine before reboot.
```

15. CD-ROMを取り出し、再起動します。再起動後、必要なLANケーブルを接続してください。

```
# cd
# eject
# shutdown -r now
```

● セキュリティポリシーをインストール

セキュリティポリシーの再インストールについて説明します。

1. SmartDashboardから管理サーバへ接続し、FireWall-1管理サーバとFirewall本体との通信を行うための設定を行う。

   FireWall-1管理サーバとFirewall本体との通信を行うための設定については、本章の「セキュリティポリシーの設定」-「Firewallオブジェクトの作成」を参照してください。

2. Firewall本体へセキュリティポリシーをインストールする。

3. 運用系Firewall、待機系Firewallの順で再起動する。

注意・制限事項

- Firewall本体が2台以上必要です。 また、ライセンスは同じユーザー数のものをそれぞれの実IPアドレスで申請する必要があります。
- 自動フェイルバック時、接続されていたセッションが切断される場合があります。
- フェイルオーバが発生した場合、IKEセッションは失われる可能性があります。
- 自動フェイルバックが設定されている場合、運用系サーバ再起動後、自動的に運用系サーバで業務が開始されます。自動フェイルバックが設定されていない場合は、待機系サーバで業務が起動されたままになり、運用系サーバの方が待機状態になります(運用系、待機系の逆転)。運用系サーバに業務を切り替える場合はコマンド(clpgrp-m)によりサーバの切り替えを実行する必要があります。
- 待機系で監視対象IPアドレスとの通信途絶が発生している場合、運用系でリソース異常が発生しても待機系サーバに業務は引き継がれません。ただし、この場合でもコマンド(clpgrp-m)により業務実行サーバを切り替えることは可能です。

~Memo~